(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 197 52 853 C 1**

(51) Int. Cl.[6]: G 06 F 11/00

(21) Aktenzeichen: 197 52 853.8-53
(22) Anmeldetag: 28. 11. 97
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 11. 2. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens Nixdorf Informationssysteme AG, 33106 Paderborn, DE

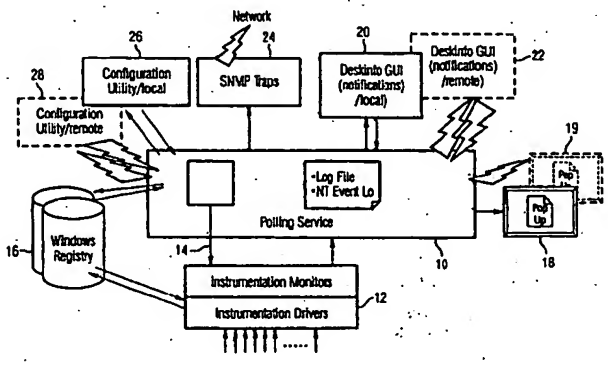
(74) Vertreter:
Epping, W., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 82131 Gauting

(72) Erfinder:
Bräuer, Joachim, Dipl.-Ing. (FH), 86399 Bobingen, DE; Munker, Thomas, 86152 Augsburg, DE; Palatzky, Markus, Dipl.-Ing. (FH), 86316 Friedberg, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 40 39 013 C2
LEMME, Helmuth: Vorbeugen statt Reparieren, in: Elektronik 21/1996, S. 58-60, 62, 64, 65;

(54) Verfahren und System zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern

(57) Beschrieben wird ein Verfahren und ein System zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern. Ein konfigurierbares Alarmfilter verteilt Alarmmeldungen an verschiedene Schnittstellen (18 bis 24) im Rechnerverbund. Durch eine Konfigurationsroutine werden Parameter des Alarmfilters festgelegt.



DE 197 52 853 C1

DE 197 52 853 C1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern, bei dem in jedem Personal Computer Betriebszustände abgefragt werden, die zu Alarmmeldungen führen können. Ferner betrifft die Erfindung ein System, welches das genannte Verfahren realisiert.

Personal Computer können während des Betriebs unterschiedliche Betriebszustände einnehmen. Diese Betriebszustände werden durch verschiedene Sensoren und Auswerteeinrichtungen signalisiert. Beispielsweise kann ein Deckelsensor vorgesehen sein, der mitteilt, ob das Gehäuse des Personal Computers geschlossen ist. Ferner ist es aus der Zeitschrift "Elektronik 21/1996": Seiten 58 bis 60, 62, 64, 65 bekannt, durch Sensoren überwachen zu lassen, ob ein Lüfter im Personal Computer vorhanden ist, ob dieser bereits eine hohe Betriebsdauer hinter sich hat oder ausgefallen ist. Weitere Überwachungen betreffen die Betriebstemperatur, das Vorliegen von Spannungen innerhalb vorgegebener Toleranzbereiche, das Vorhandensein eines Kurzschlusses in einem Bus-System, die Drehzahl einer Festplatte oder deren Fehlerrate, etc.

Aus DE 40 39 013 C2 ist eine Datenverarbeitungsanlage mit mehreren Prozessoren bekannt, die Einrichtungen zur Erfassung von Informationen über Fehlerfunktionen aufweist, wobei im Falle eines ersten Fehlermeldesignals diejenigen Teile der Datenverarbeitungsanlage gestoppt werden, die den Fehler verursacht haben, ferner die Folgefehler unterbunden werden und schließlich die für eine Fehlerbehebung erforderlichen Informationen erfaßt werden.

Beim Wechsel von einem Betriebszustand in den anderen kann es zu Funktionsstörungen im Personal Computer oder im Rechnerverbundnetz kommen. Eine solche Störung wird nach dem Stand der Technik dem Benutzer, dem Systemverwalter oder Administrator durch entsprechende Meldungen mitgeteilt. Bei bekannten Verfahren bzw. Systemen, wie z. B. dem SNI Server View der Siemens Nixdorf Informationssysteme AG, der Compaq Intelligent Manageability der Firma Compaq und dem Intel LAN-Desk Client Manager V3.1 der Firma Intel, werden Sensoren und Statuselemente, sogenannte Instrumentation Monitors, der betreffenden Funktionseinheiten, z. B. einer Festplatte, in einem Polling-Verfahren in bestimmten Zeitabständen abgefragt. Die Zeitabstände zwischen zwei Abfragen kann mithilfe einer Software eingestellt werden. Ferner können Schwellwerte für analoge Größen festgelegt werden, um Schwellwertüberschreitungen zu erkennen, beispielsweise bei der Spannungsüberwachung. Bestimmte Betriebszustände führen dann zu einer Fehlermeldung, die vom Benutzer oder Administrator auszuwerten ist. Innerhalb eines Rechnerverbundnetzes kann nun eine Vielzahl von Alarmmeldungen auftreten, die das gesamte System unübersichtlich machen. Es wäre daher wünschenswert, Alarmmeldungen selektiv an den Orten anzuzeigen, wo sie von einem Benutzer sinnvoll ausgewertet werden können.

Es ist Aufgabe der Erfindung, ein Verfahren und ein System zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz so auszubilden, daß, abhängig von einer Überprüfung einzelner Alarmmeldungen, eine gezielte Auswertung der jeweiligen Alarmmeldung sowie eine entsprechende Einflußnahme auf das Rechnerverbundnetz möglich ist.

Die Lösung dieser Aufgabe ergibt sich erfindungsgemäß durch die Merkmale des Anspruchs 1. Vorteilhafte Weiterbildungen der Erfindung sind in Unteransprüchen angegeben.

Durch die Einschaltung eines Alarmfilters, welches softwaretechnisch realisiert ist, kann eine gezielte Auswahl von Alarmmeldungen und eine entsprechende Verteilung an die verschiedenen Schnittstellen im Rechnerverbund erfolgen. Auf diese Weise kann auch in einem komplexen Rechnerverbundnetz eine übersichtliche Darstellung von Alarmmeldungen erreicht werden, insbesondere, indem Alarmmeldungen unterdrückt werden.

Beispielsweise ist es möglich, bestimmte Alarmmeldungen nur an den Administrator Personal Computer zu übertragen, während am betroffenen Personal Computer sämtliche Schnittstellen diese Alarmmeldungen erhalten. Auch kann je nach Schweregrad des Alarms eine Auswahl von Schnittstellen getroffen werden, so daß sehr flexibel auf unterschiedliche Betriebszustände reagiert werden kann.

Gemäß einem Ausführungsbeispiel der Erfindung wird die Konfigurationsroutine am betreffenden Personal Computer oder über einen Remote-Zugriff innerhalb des Rechnerverbundnetzes ausgeführt. Ein solcher Remote-Zugriff kann beispielsweise von einem anderen Personal Computer aus erfolgen, vorzugsweise jedoch vom Administrator Personal Computer.

Vorzugsweise werden Personal Computer im Rechnerverbundnetz mit gleicher Konfiguration zu einer Gruppe zusammengefaßt. Die jeweilige Weiterleitung oder Nichtweiterleitung der Alarmmeldungen für diese Gruppe wird durch eine einzige Konfigurationsroutine festgelegt. Auf diese Weise kann der Konfigurationsaufwand verringert werden, ohne daß die Flexibilität der Auswahl von Alarmmeldungen beeinträchtigt wird.

Gemäß einem anderen Ausführungsbeispiel werden die Konfigurationsdaten im jeweiligen Personal Computer lokal in der Registry-Datenbank des Betriebssystems gespeichert, beispielsweise im Betriebssystem Windows NT. Diese Registry-Datenbank dient zur Konfiguration des gesamten Personal Computers. In ihr werden alle für das Betriebssystem und seine Programme relevanten Software- und Hardwareeinstellungen gespeichert. Von der Registry-Datenbank werden durch das Betriebssystem automatisch Sicherheitskopien angefertigt, um im Falle einer Beschädigung schnell auf Ersatzdaten zugreifen zu können. Durch dieses Ablegen der Konfigurationsdaten in dieser Registry-Datenbank werden die Sicherungsfunktionen des Betriebssystems für diese Konfigurationsdaten genutzt.

Gemäß einem weiteren Aspekt der Erfindung wird ein System zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern angegeben, welches das vorgenannte Verfahren realisiert. Dieses System ist durch die Merkmale des Anspruchs 11 definiert. Vorteilhafte Weiterbildungen sind in den darauffolgenden Ansprüchen angegeben. Durch das System werden ebenfalls die beim bereits erläuterten erfindungsgemäßen Verfahren erreichten Vorteile erzielt.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der Zeichnung erläutert. Darin zeigt

Fig. 1 eine Blockdarstellung wichtiger Funktionseinhegten eines Personal Computers im Rechnerverbundnetz, und

Fig. 2 eine Matrix, mit deren Hilfe Konfigurationsdaten festgelegt werden.

Fig. 1 zeigt schematisch verschiedene Funktionseinheiten eines Personal Computers, die bei der Erfindung genutzt werden. Als Betriebssystem wird hier Windows NT der Firma Microsoft eingesetzt. In einem Funktionsblock **10** des Betriebssystems wird der Polling-Service realisiert, gemäß dem an einen Überwachungsbaustein **12** Abfragetakte über den Datenweg **14** ausgegeben werden. Der Überwachungsbaustein **12** enthält Treiberbausteine, die Signale von Sensoren, die die Betriebszustände des Personal Computers und gegebenenfalls des Netzes erfassen, an einen Monitorbau-

stein weitergeben. Dieser Monitorbaustein bereitet die Meldungen auf und gibt sie an den Funktionsblock **10** weiter, wo sie in entsprechenden Dateien abgespeichert werden, beispielsweise im betriebssystemspezifischen LOG FILE und im NT EVENT LOG. Konfigurationsdaten des Überwachungsbausteins **12** sind in der Registry-Datenbank **16** enthalten, welche zum Betriebssystem Windows NT gehört.

Der Funktionsblock **10** bedient verschiedene Informationsschnittstellen **18** bis **24**. Die Schnittstelle **18** ist ein Warnungsfenster, das auch als Pop Up bezeichnet wird, wobei beim Auftreten einer Alarmmeldung ein Fenster am Bildschirm erscheint, in welchem Informationen über die Alarmmeldung angezeigt werden. Das Warnungsfenster **18** ist lokal angelegt, d. h. es werden am lokalen Personal Computer Informationen angezeigt. Eine andere Möglichkeit besteht darin, in einem entfernten Warnungsfenster **19** diese Meldung anzuzeigen, d. h. im allgemeinen unter Nutzung des Rechnerverbundnetzes.

Eine weitere Schnittstelle ist die grafische Deskinformations-Schnittstelle **20**, welche eine lokale Schnittstelle ist. Bei der Deskinformations-Schnittstelle **20** werden in einem grafischen Userinterface (GUI) sämtliche möglichen Alarmmeldungen angezeigt. Die aktuelle Alarmmeldung erscheint in dieser Darstellung abgehoben, beispielsweise durch eine bestimmte Farbdarstellung. Weiterhin können die Informationen über eine entfernte Deskinformations-Schnittstelle **22** angezeigt werden, beispielsweise auf einem weiteren Personal Computer des Rechnerverbundnetzes. Die Deskinformations-Schnittstelle ist eine Entwicklung der Siemens Nixdorf Informationssysteme AG.

Eine weitere Schnittstelle ist als SNMP-Traps-Schnittstelle **24** definiert. Über diese Schnittstelle **24** können mit Hilfe des Rechnerverbundnetzes die Alarmmeldungen an weitere Personal Computer (SNMP-Konsolen) weitergegeben werden. Diese Personal Computer zeigen grafische Informationen über die Alarmmeldungen an.

Zur Konfigurierung des Alarmfilters, welches innerhalb des Funktionsblockes **10** realisiert ist, ist ein lokales Konfigurationsmodul **26** oder ein entferntes Konfigurationsmodul **28** vorgesehen. In den Konfigurationsmodulen **26**, **28** werden in einem Dialog die Konfigurationsdaten festgelegt. Das Alarmfilter legt auf Grundlage dieser Konfigurationsdaten fest, an welche Schnittstelle des betreffenden Personal Computers oder an Schnittstellen im Rechnerverbundnetz die jeweilige Alarmmeldung weitergeleitet oder eine Weiterleitung der Alarmmeldung unterbunden wird.

Fig. 2 zeigt anhand einer Darstellung das Festlegen der Konfigurationsdaten für einen speziellen Personal Computer oder für eine Gruppe von Personal Computern. In einer Matrix sind in einer ersten Spalte die verschiedenen Betriebszustände eingetragen, die zu Alarmmeldungen führen können. Im vorliegenden Fall sind Alarme eines Administrator Personal Computers dargestellt. In einer zweiten Spalte ist angegeben, ob die Alarmmeldungen auf der lokalen Deskinformations-Schnittstelle **20** gemäß **Fig. 1** ausgegeben werden sollen. Im vorliegenden Fall wird dies für sämtliche Alarmmeldungen bejaht. Selbstverständlich können einzelne Alarmmeldungen auch unterdrückt sein – es erscheint dann in dieser Spalte anstelle eines Ja-Eintrags ein Nein-Eintrag. Die dritte Spalte betrifft die Schnittstellen, die als Ereignisanzeige ausgebildet sind. Diese Ereignisanzeigen werden aus der Datei NT EVENT LOG gemäß Funktionsblock **10** in **Fig. 1** abgeleitet.

Eine vierte Spalte der Matrix nach **Fig. 2** betrifft die Schnittstelle Protokolldarstellung, die auf Daten im LOG-FILE des Betriebssystems Windows NT zugreifen. Schließlich ist eine fünfte Spalte vorgesehen, die Konfigurationsdaten für die Schnittstelle Warnungsfenster zuständig sind. Diese Schnittstelle ist gemäß **Fig. 1** in dem Block **18** realisiert.

Das Einstellen der Konfigurationsdaten anhand der in **Fig. 2** gezeigten Matrix erfolgt entweder durch Mouseklick auf einem Kreuzungspunkt, wobei jeweils ein Umschalten von Ja nach Nein erfolgt. Eine andere Möglichkeit besteht darin, mittels der Mouse den Anfang einer Zeile oder den Anfang einer Spalte anzuwählen, um den Kreuzungspunkt in der Matrix zu definieren. Durch Mouse-Klick auf ein voreingestelltes Matrixelement, beispielsweise in der linken oberen Ecke der Matrix, kann die gesamte Matrix weitergeschaltet werden.

Wie erwähnt, können Personal Computer mit gleicher Konfiguration zu Gruppen zusammengefaßt werden. In einem solchen Fall können die Personal Computer einer Gruppe durch eine einzige Konfigurationsmatrix eingestellt werden. Das Konfigurieren kann vom lokalen Personal Computer oder von einem entfernten Personal Computer des Rechnerverbundnetzes vorgenommen werden, vorzugsweise durch den Administrator Personal Computer. Weiterhin kann die Matrix ergänzt sein, indem einzelne Personal Computer angegeben werden, deren grafische Schnittstelle angewählt wird, um Alarmmeldungen des Rechnerverbundnetzes anzuzeigen. Wie leicht zu erkennen ist, können aufgrund der matrixförmigen Darstellungen, einzelne Alarm-Klassen für alle Schnittstellen, einzelne Schnittstellen für alle Alarm-Klassen, sämtliche Alarm-Klassen und Schnittstellen gleichzeitig für einen einzelnen Personal Computer oder eine Gruppe von Personal Computern eingestellt werden. Es ist somit jede beliebige Kombination von Einstellungen für den lokalen Personal Computer wie auch für entfernte Personal Computer von einem Administrator-Arbeitsplatz möglich.

Patentansprüche

1. Verfahren zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern,
bei dem in jedem Personal Computer Betriebszustände abgefragt werden, die zu Alarmmeldungen führen können,
bei Auftreten einer Alarmmeldung diese durch ein konfigurierbares Alarmfilter überprüft wird und abhängig von dieser Prüfung die Alarmmeldung an eine Schnittstelle (**18** bis **24**) im Rechnerverbund weitergeleitet oder die Weiterleitung der Alarmmeldung unterbunden wird,
und bei dem in einer Konfigurationsroutine für das jeweilige Alarmfilter die Weiterleitung oder die Nichtweiterleitung der Alarmmeldungen festgelegt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Konfigurationsroutine am betreffenden Personal Computer oder über einen Remote-Zugriff innerhalb des Rechnerverbundnetzes ausgeführt wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß Personal Computer im Rechnerverbundnetz mit gleicher Konfiguration zu einer Gruppe zusammengefaßt werden und die jeweilige Weiterleitung oder Nichtweiterleitung der Alarmmeldungen für diese Gruppe durch eine einzige Konfigurationsroutine festgelegt wird.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle im Rechnerverbund eine Deskinformations-Schnittstelle (**20**, **22**) verwendet wird, bei der in einem grafischen Userinterface sämtliche möglichen Alarmmeldungen angezeigt werden und die aktuelle Alarmmeldung in

der Darstellung abgehoben erscheint.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle eine Protokolldarstellung verwendet wird, bei der die aktuelle Alarmmeldung gegebenenfalls mit weiteren Informationen angezeigt wird, wobei auf eine LOG-Datei zugegriffen wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle eine Ereignisanzeige verwendet wird, bei der Daten der Datei EVENT LOG des Betriebssystems WINDOWS NT angezeigt werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle ein Warnungsfenster (**18, 19**) verwendet wird, gemäß dem beim Auftreten einer Alarmmeldung ein Fenster am Bildschirm erscheint, in welchem Informationen über die Alarmmeldung angezeigt werden.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Konfigurationsdaten im jeweiligen Personal Computer lokal in der Registry-Datenbank (**16**) des Betriebssystems WINDOWS NT gespeichert werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur Konfigurierung sämtliche Alarmmeldungen sowie die möglichen Schnittstellen (**18** bis **24**) als Matrix dargestellt werden und daß beim Konfigurieren an den Kreuzungspunkten von Zeilen und Spalten der Matrix Entscheidungsdaten eingegeben werden, die bei der Prüfung der Alarmmeldungen ausgewertet werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Konfigurierung der verschiedenen Personal Computer oder der Gruppen von Personal Computern im Rechnerverbundnetz am Administrator-Personal Computer vorgenommen wird.

11. System zum Verarbeiten von Alarmmeldungen in einem Rechnerverbundnetz mit mehreren Personal Computern,
mit einem Überwachungsbaustein (**12**) in jedem Personal Computer, der Betriebszustände abfragt, die zu Alarmmeldungen führen können,
mit einem konfigurierbaren Alarmfilter, das bei Auftreten einer Alarmmeldung diese überprüft und abhängig von dieser Prüfung die Alarmmeldung an eine Schnittstelle (**18** bis **24**) im Rechnerverbund weiterleitet oder die Weiterleitung der Alarmmeldung unterbindet,
wobei Konfigurationsdaten für das jeweilige Alarmfilter festlegbar sind, anhand denen die Weiterleitung oder die Nichtweiterleitung der Alarmmeldungen erfolgt.

12. System nach Anspruch 11, dadurch gekennzeichnet, daß die Konfigurationsroutine am betreffenden Personal Computer oder über einen Remote-Zugriff innerhalb des Rechnerverbundnetzes ausgeführt wird.

13. System nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß Personal Computer im Rechnerverbundnetz mit gleicher Konfiguration zu einer Gruppe zusammengefaßt sind und die jeweilige Weiterleitung oder Nichtweiterleitung der Alarmmeldungen dieser Gruppe durch eine einzige Konfigurationsroutine die jeweilige Weiterleitung oder Nichtweiterleitung der Alarmmeldungen festlegbar ist.

14. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle im Rechnerverbund eine Deskinformationsschnittstelle (**20, 22**) vorgesehen ist, bei der in einem grafischen Userinterface sämtliche möglichen Alarmmeldungen angezeigt werden und die aktuelle Alarmmeldung in der Darstellung abgehoben erscheint.

15. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle eine Protokolldarstellung vorgesehen ist, bei der die aktuelle Alarmmeldung gegebenenfalls mit weiteren Informationen angezeigt wird, wobei auf eine LOG-Datei zugegriffen wird.

16. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle eine Ereignisanzeige vorgesehen ist, bei der Daten der Datei EVENT LOG des Betriebssystems WINDOWS NT angezeigt werden.

17. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schnittstelle ein Warnungsfenster (**18, 19**) vorgesehen ist, gemäß dem beim Auftreten einer Alarmmeldung ein Fenster am Bildschirm erscheint, in welchem Informationen über die Alarmmeldung angezeigt werden.

18. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Konfigurationsdaten im jeweiligen Personal Computer lokal in der Registry-Datenbank (**16**) des Betriebssystems WINDOWS NT gespeichert sind.

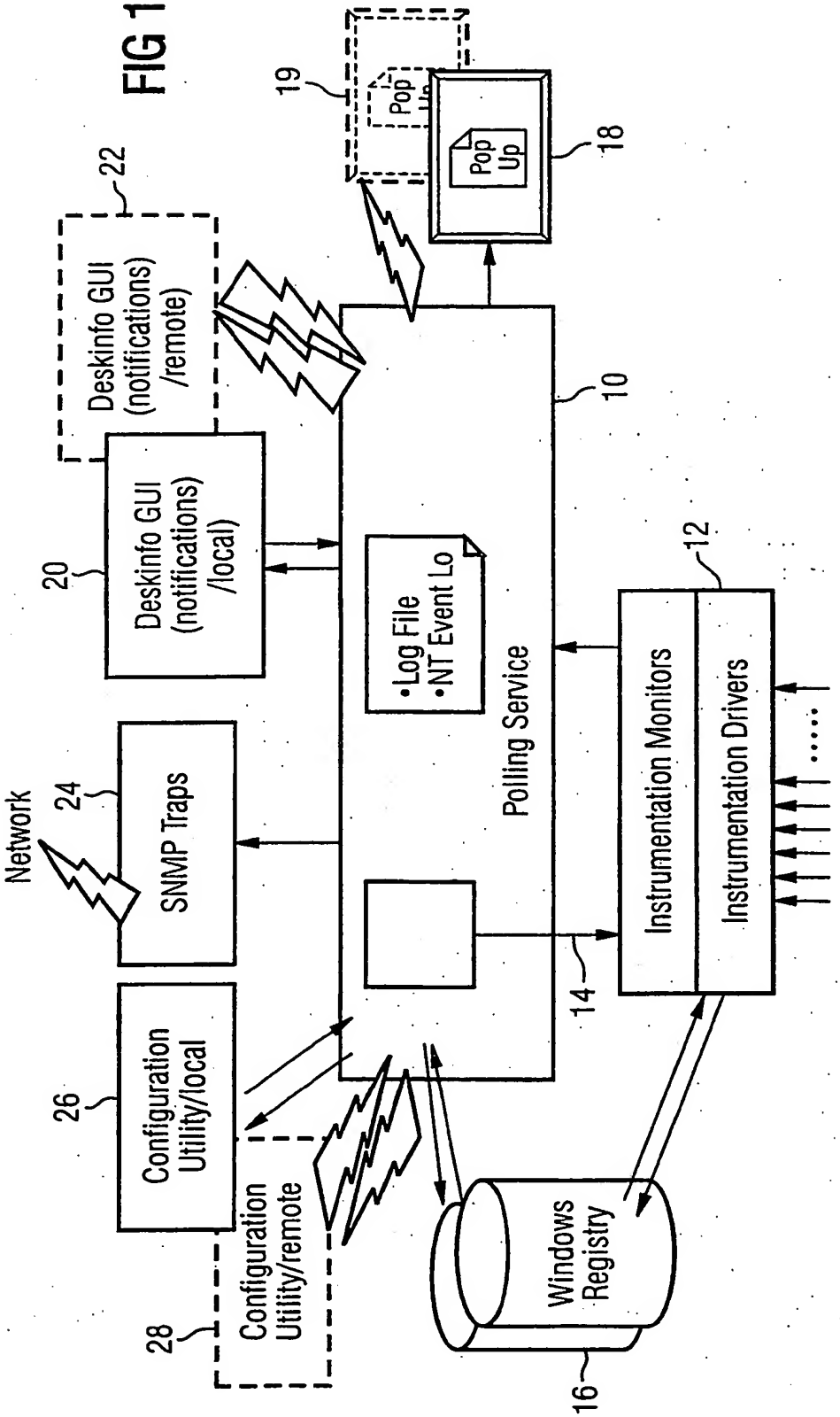
19. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur Konfigurierung sämtliche Alarmmeldungen sowie die möglichen Schnittstellen als Matrix darstellbar sind und daß beim Konfigurieren an den Kreuzungspunkten von Zeilen und Spalten der Matrix Entscheidungsdaten eingegeben werden, die bei der Prüfung der Alarmmeldungen ausgewertet werden.

20. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Konfigurierung der verschiedenen Personal Computer oder der Gruppen von Personal Computern im Rechnerverbundnetz am Administrator-Personal Computer vornehmbar ist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 197 52 853 C1
Int. Cl.[6]: G 06 F 11/00
Veröffentlichungstag: 11. Februar 1999

FIG 1



Nummer: DE 197 52 853 C1
Int. Cl.[6]: G 06 F 11/00
Veröffentlichungstag: 11. Februar 1999

FIG 2

(12) UK Patent Application (19) GB (11) 2 325 548 (13) A

(43) Date of A Publication 25.11.1998

(21) Application No 9710471.5

(22) Date of Filing 21.05.1997

(51) INT CL[6]
G08B 25/08 29/12

(52) UK CL (Edition P)
G4H HNLB HTG H1A H13D H14A H14G H60
U1S S1931 S1978 S2166 S2181 S2188 S2206 S2207

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition P) G4H HNHE HNLA HNLB
INT CL[6] G08B
ONLINE:WPI

(71) Applicant(s)
Richard Parviz Nabavi
Clayton's Farmhouse, Newick Lane, MAYFIELD,
E Sussex, TN20 6RE, United Kingdom

(72) Inventor(s)
Richard Parviz Nabavi

(74) Agent and/or Address for Service
Withers & Rogers
4 Dyer's Buildings, Holborn, LONDON, EC1N 2QP,
United Kingdom

(54) Abstract Title
Security alarm systems

(57) A Security Alarm System Controller 1 comprises input means for receiving data from at least one detector 4,5 which indicates a breach of security, output means for outputting an alarm signal, and computer network server means operable to interact between the controller and a computer network user 9 who has access to the network (e.g. Internet) 11. The computer network server means is operable to pass data relating to the status of the alarm system to the network user 9 and to re-configure the alarm system controller on the basis of instructions from the network user 9.

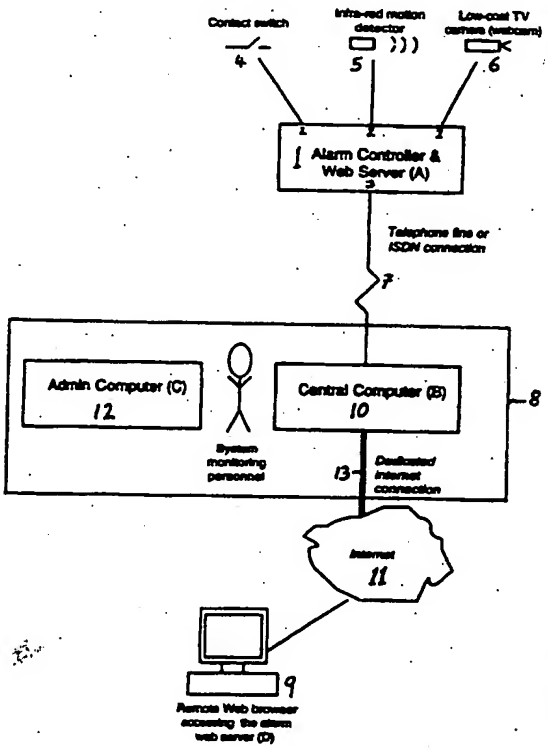


Figure 1: How the alarm controller/web server links via the Security Centre to the Internet and hence to the remote user

GB 2 325 548 A

The claims were filed later than the filing date within the period prescribed by Rule 25(1) of the Patents Rules 1995

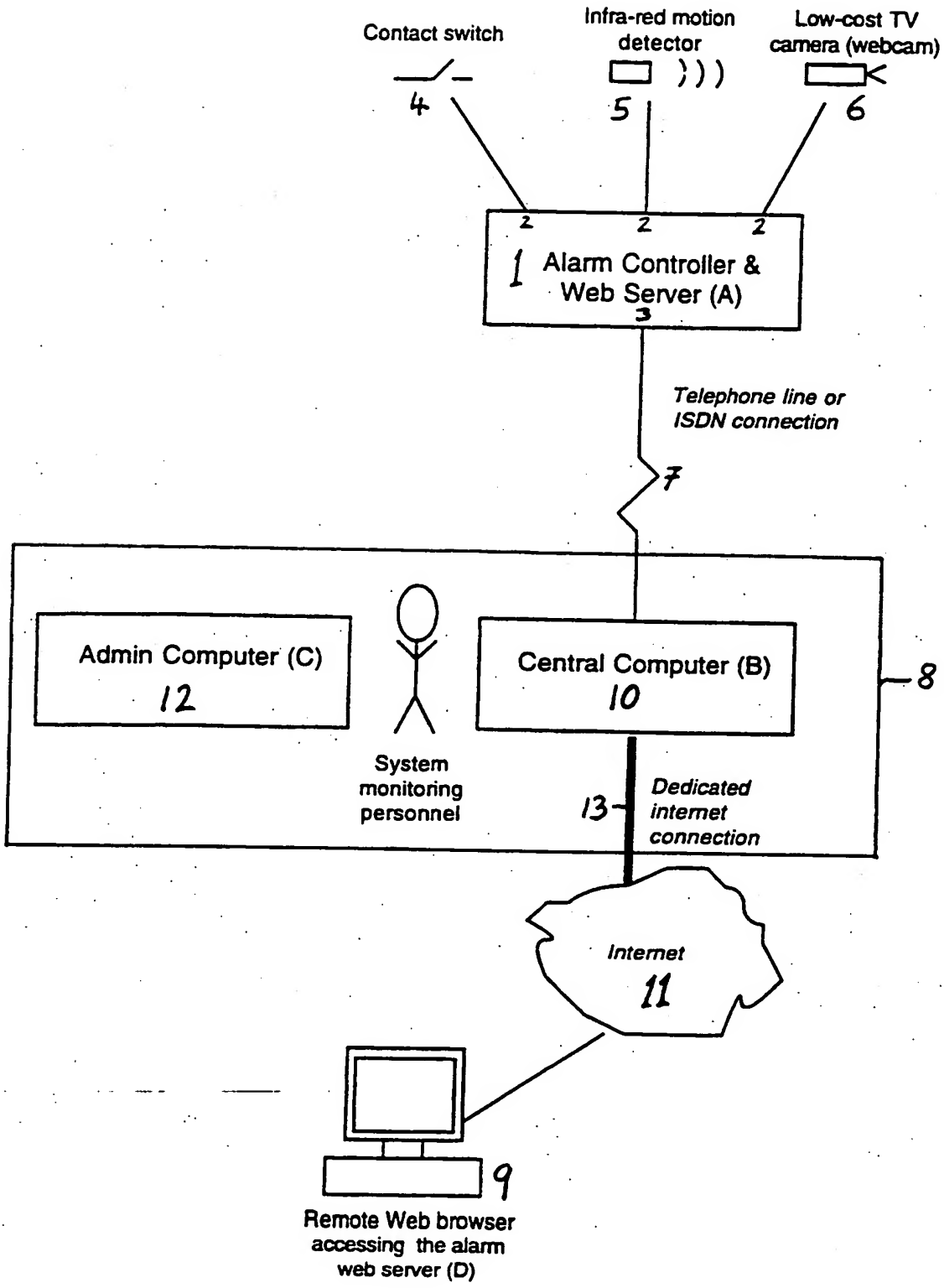


Figure 1: How the alarm controller/web server links via the Security Centre to the internet and hence to the remote user

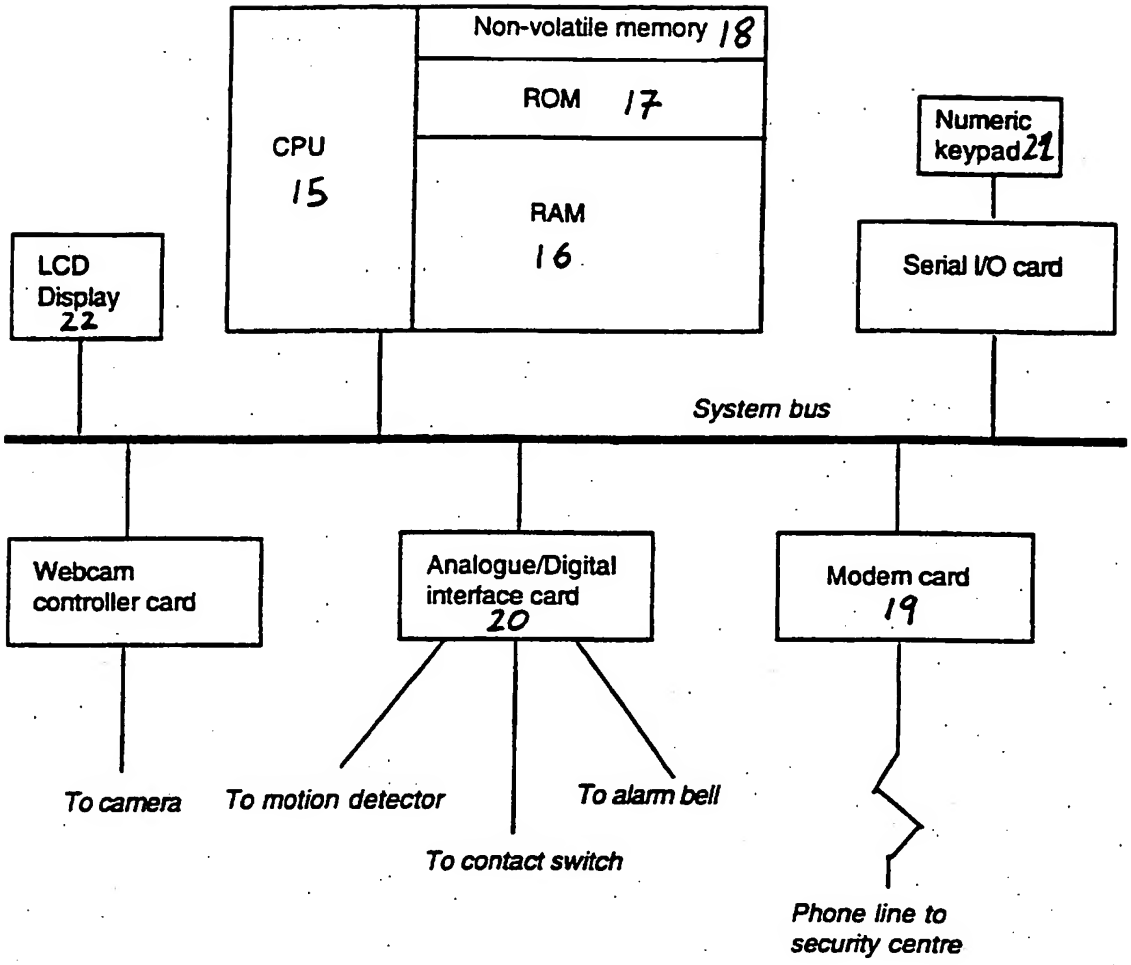


Figure 2: Main hardware components in an implementation of the controller unit

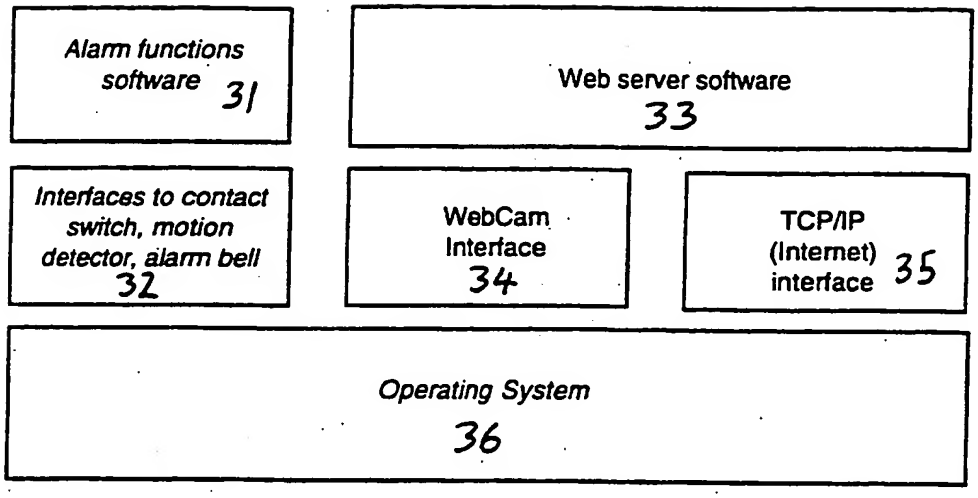


Figure 3. The main software components in the alarm controller. The elements shown in italics are similar to those needed in a conventional alarm controller, although the operating system is likely to be more sophisticated here

IMPROVEMENTS IN AND RELATING TO SECURITY ALARM SYSTEMS AND THEIR CONTROLLERS

This invention relates to security alarm systems, for example those which are used to protect buildings, and to their controllers.

Existing security alarm systems comprise an alarm controller, detectors (such as door and window switches, pressure pads and movement detectors) which monitor a property, and a bell or siren which is activated by the controller when security is breached. Many countries now have legislation which only permits the use or fitting of such an alarm provided that the controller notifies a keyholder or central monitoring station of the breach of security, and this is normally achieved by the controller having access to a telephone line.

Once a person has left the property, it is common for that person to worry that he or she has forgotten to set the alarm system, or to close alarmed doors which might cause the bell or siren to sound or prevent the system from setting.

Hitherto, it has been necessary to telephone a neighbour or other keyholder, or perhaps the central monitoring station, to ask them to check the property. This is clearly an unsatisfactory situation which no-one has addressed, despite the problem having existed for some years.

Accordingly, the present invention is a security alarm system controller for controlling an alarm system, the controller comprising input means for receiving data from at least one detector which indicates a breach of security, output means for outputting an alarm signal, and computer network server means operable to interact between the security alarm controller and a computer network user who has access to the network, whereby the computer network server means is operable to pass data relating to the status of the alarm system to the network user and is operable to re-configure the alarm system on the basis of instructions from the network user. The network is preferably the Internet because it can be accessed from practically everywhere. Thus, it is possible for a person to check his or her alarm system remotely via the Internet or other network in order to find out whether or not it is set, and if, for example, it is found that it has not been set, the person can then set it. In addition, if the alarm detectors are arranged to protect the

property in zones, the zone configuration can be altered, for example to exclude a particular zone if an alarmed internal door has been left open. It is particularly advantageous to use a telephone line connection to gain access to the controller, partly because it is cheap, and few buildings now do not have telephone lines, and partly because most controllers have access to a telephone line anyway so as to alert a central monitoring station of any breach of security. It is clearly advantageous to use the same telephone line as that used to alert the central monitoring station.

It is also advantageous if access to the controller by an Internet user is only possible if the user goes through a computer at the central monitoring station. This makes the Internet web server more secure from unauthorised web users, particularly if the central monitoring station has an access authorisation system for permitting only authorised access. If the web user is not given the location of the secure property, anyone who might gain unauthorised access cannot identify the property.

Many people, especially when they are away from home for a long period, would like to observe their own home to reassure them that it is safe. If the security alarm system includes one or more cameras, the image data from them can be accessed via the Internet, so that a person can see live images of his or her home. If the or each camera includes means for re-directing its position, the web server means would be able to control the re-directing means on the basis of instructions received from a web user. The re-directing means might include motors for changing the angle at which the or each camera is inclined relative to a support. A person can then direct the or each camera remotely via the Internet to scan the property so that the person can see that it is secure and safe.

In another aspect of this same invention, a security alarm system comprises: a controller having input means for receiving data from at least one detector which indicates a breach of security, and output means for outputting an alarm signal; a computer network server means located as part of the controller or entirely separate therefrom which is operable to interact between the security alarm controller and a computer network user who has access to the network, whereby the network server means is operable to pass data relating to the status of the alarm system to the network user, and is operable to re-configure the alarm system on the basis of instructions from the network user. The preferred network is the Internet since this is accessible from all over the world. The

network server means could be located at a central monitoring station run by a security company so that a single network server means can be used to interact with many different properties having security alarms. The network server means will typically use telephone lines to communicate with individual controllers so as to receive information relating to the security of the property and to send instructions to the controllers.

Embodiments of the invention are described below, by way of example only, with reference to the accompanying drawings, in which:-

Figure 1 is a schematic diagram of the security alarm system and its connections;

Figure 2 is a schematic diagram showing the general arrangement of hardware components of the alarm controller; and

Figure 3 is a block diagram showing the software which controls the hardware.

Figure 1 shows a security alarm system in which an alarm controller 1 includes one or more input means 2 and an output means 3. The input means 2 are connected to various sensors or detectors which detect breaches of security of, for example, a home. Two types of detectors are shown, a contact switch 4, which would typically be fitted to a door or window for detecting whether or not the door or window is open, and an infra-red motion detector 5 which would normally be fitted in an upper corner of a room, hall or landing for detecting movement within that room. A low-cost television camera 6 could be placed in a room, positioned so as to observe activity in that room. The camera could be positioned so as to observe garages, stables, sheds or even the outside of a house. This is also connected to the input means 2. Other types of detectors could also be used, but the contact switch detector 4 and the infra-red motion detector 5 are particularly favoured detectors since they are relatively cheap and effective. The television camera 6 is also very good, but tends to be more expensive. The detectors produce detector data which is fed into the input means 2 of the controller 1, and the data from the television camera 6 is in the form of image data. The detectors are normally connected to the input means 2 by cables, but might be cordless detectors which send their data to the controller by radio waves or other cordless methods.

The output means 3 includes a telephone line or ISDN link 7. If a breach of security is detected by a detector, the alarm controller 1 accesses the line 7 and notifies a central monitoring station 8 where personnel are warned of the breach. The personnel

may then take appropriate action, for example sending a security guard to the home to investigate, and possibly calling the police to the home.

The alarm controller 1 also includes Internet web server means in addition to the part of the alarm which monitors the detectors and contacts the central monitoring station 8. This enables a person to access the controller 1 from a remote Internet web terminal 9. In this embodiment, the Internet connection to the controller 1 is achieved using the same telephone or ISDN connection 7 as above. Thus the Internet user must access the controller 1 through a computer 10 at the central monitoring station 8. The computer 10 includes means for controlling the access of an Internet user to the controller 1. Thus, before an Internet user gains access to the controller 1, it is necessary for him to identify himself as an authorised person. Anyone who gains access to the controller 1 from the Internet 11 does not receive any information as to the location of the home since, in the unlikely event that an unauthorised person gained access, they could de-activate all or part of the alarm system. The information as to the location of the home is kept on a second, separate computer 12 which only the personnel at the central monitoring station 8 have access to.

The computer 10 has a dedicated connection 13 to the Internet 11, and the Internet user is able to access the computer 10 simply using a standard computer with web browsing software, for example Netscape Navigator (Trade Mark) or Microsoft Internet Explorer (Trade Mark). The computer may be a standard desktop P.C. or other consumer electronics device with Internet access, such as an adapted television, for example WebTV (Trade Mark). Such a unit might be found in homes, offices or hotel rooms. A user could even use a portable computer coupled with a mobile telephone.

The security alarm system controller 1 is microcomputer based and runs an operating system which is capable of running web server software. Referring to Figure 2, the controller 1 includes a microprocessor 15, Random Access Memory (RAM) 16, Read-Only Memory (ROM) 17, and a small amount of battery-backed-up or non-volatile "flash" memory 18 which would hold configurations and password information even if power were lost for an extended period. A modem 19 is included for communicating with the computer 10 of the central monitoring station 8, and interface circuitry 20 for connecting the controller 1 to the alarm circuit contact switch 4, infra-red detectors 5,

cameras 6 and an alarm bell (not shown) and to any supplementary devices connected to the controller. A screen and keyboard would not normally be necessary, but instead a simple keypad interface 21 device might be used to enter a security code when enabling or disabling the alarm, and an LCD display (or indicator lights) 22 which show the state of the system.

Figure 3 shows the main software elements required, including alarm function software 31 which handles the enabling and disabling of the alarm, the monitoring of the detectors, and the triggering of the alarm bell (and alerting the central monitoring station) when an incident occurs. Interface software 32 enables the processor to detect changes of state the detectors and the camera and also controls the alarm bell or siren. Web server software 33 displays the state of the alarm controller 1 in the form of web "pages" to the user and also allows the user, to change settings, such as whether the alarm, or just a circuit of the alarm, is enabled or disabled. It also displays the image data from the or each camera 6 as pictures, possibly held as JPEG type images within the web pages. Camera interface software 34 permits the receiving of image data from the camera or cameras 6 and the storing of the image data as JPEG images ready for the web server software 33. TCP/IP interface software Internet 35 permits the controller 1 communicate with the central monitoring station, and with e remote web user. The operating system 36 should be a real time operating system such as OS/9 (Trade Mark), and the web server software 33 can be based on commercially available products such as Spyglass Micro Server (Trade Mark). The operating system 36, the web server software 33 and the control software for the alarm system would typically be held in the ROM 17, but might be held on disk.

If a detector such as a contact switch or an infra-red motion detector detects a breach of the security of the home, the controller 1 will receive this information in the form of an alarm signal. The controller 1 then raises the alarm, usually by setting off a bell or siren which alerts neighbours and passers-by, and should scare away any person attempting to enter the house. In addition, in some places, legislation demands that home security alarms should make a keyholder aware of the alarm when it has been set off. This is often done by a central monitoring station 8 which is connected to the alarm controller by the telephone line or ISDN connection 7.

The operation of the security alarm system will now be described by reference, in particular to Figure 1, but also to Figures 2 and 3.

When a person leaves his home, he will set the security alarm, but it is common that such a person, once he has travelled some distance from his home will not be able to remember whether or not he has actually set the alarm or not. In addition, he might be also be worried that he has not secured the property, for example, closing all of the doors and windows. By using this invention, the person can use any Internet web terminal such as a P.C. as described above, to contact the central monitoring station 8. Once he has access to the computer 10 of the central monitoring station 8, he must identify himself as a person authorised to access the alarm controller 1. This may be done by passwords or other systems of authorisation. The computer 10 of the central monitoring station 8 establishes a secure link or "socket" with the remote web terminal 9, i.e. A encrypted link, and this can also be used to verify the identify of the user. A second verification stage might also be built into the alarm controller 1. All data passed between the web user's terminal 9 and the controller 1 would be protected by a secure socket link so that, even after the connection has been established, it would be difficult to "hack" into the communication system between the user and the alarm system controller. The computer 10 does not include any information regarding the address of the home or its owner. This is because, in the unlikely event that an unauthorised person would gain access to the alarm controller, not only might they be able to identify valuable items within the home using the television camera 6, they might also be able to disable the alarm controller prior to burgling the property. When the central monitoring station 8 dials up the controller 1, the telephone number would not be stored in the computer 10 since this could indicate the location of the property. A separate dial-out computer is therefore used which might dial only on the basis of an internal identification code.

If the user correctly identifies himself and is authorised access to the alarm controller, a telephone line or ISDN connection is established between the central computer and the output means 3 of the controller 1 so that the user then has access to the webserver part of the alarm controller 1. The webserver part of the alarm controller 1 is arranged so as to present itself in the form of web pages. The web pages and the controller may be operated by selecting functions using a mouse or buttons, and by using

hypertext links on the pages. The Internet user can then check the status of the controller in order to check that he has properly secured the property, closing all doors and windows, and to check to see that no one has breached the security since the alarm was set. If it has been set off, the user will be able to find out the time and which circuit or zone. If the person has not set the alarm or has not properly secured the property, he can remotely arm the alarm, or disarm certain zones of the alarm system.

In addition, where the TV camera 6 is used, the Internet user can view the images from the camera 6, thereby checking that the home is safe. This is useful where a user wishes to check that the property has not flooded or been damaged in some other way. In addition where the TV camera is motorised, the web user can operate the motors in order to re-direct the direction of the cameras. Thus, the user can scan the property. Clearly, the telephone lines used to transmit data from the camera to the Internet user will not permit high quality images to the transmitted unless the scan speed is slow. However, in such a situation, this is not normally a problem. The controller could store images, captured by the camera 6 if movement is detected while the alarm is set.

In addition, there are a number of options which might be available to the owner of such an alarm system. The security alarm system can monitor the temperature in a house left unoccupied during the winter so that the owner can check that if there is a likelihood of burst pipes during a sudden freeze. In addition, the alarm controller 1 might also be able to control other devices such as the central heating system, the lighting in the home, and the television, so that the owner can remotely make it appear that the home is occupied.

Some homes include a video entry 'phone system, and this can be connected to the alarm controller so that when people call while the owner is out, the television images from the entry 'phone can be recorded and the owner can remotely see the television images of those people who have attempted to call.

Microphones could be connected to the controller to record sounds above a certain threshold which could then be played back over the Internet to the remote user.

The system could automatically alert the Internet user, for example by a pager or by dialling a mobile telephone number, of events which are suspicious but do not justify the triggering of the alarm. For example a loud noise detected by the microphone or

movement detected by the infra-red motion detector which might have an innocent explanation.

The above embodiment describes the connection of an Internet remote terminal 9 to the alarm controller 1 only via the central monitoring station 8. While, for security reasons, this is clearly preferable, it is still possible in other embodiments for the remote web terminal to access the controller 1, directly from the Internet.

In the embodiments described above, reference is made to the Internet. However, while the Internet is the preferred computer network because is it accessible worldwide, other networks could be used.

In another embodiment (not shown) the web server is not located in the controller, but remotely therefrom. There are some advantages to locating it at the central monitoring station since a single web server can be used to access a number of controllers located at different properties. Communication between the controller and the web server can still be effected by a telephone line, and the web server can not only receive data from the controller for checking if security has been breached or if the alarm has not been set, but can also instruct the controller to re-configure the system, for example by turning the alarm on or off, or where the detectors are arranged in zones, by turning particular zones on or off. Where a camera is installed, the web server can obtain images and pass them to a web user as in the earlier embodiments. Clearly, encoded telephone signals would be used to prevent people hacking in the system. In addition, a user authorisation system should be used to ensure that only people who are authorised are permitted to contact a particular controller.

CLAIMS:

1. A security alarm system controller for controlling an alarm system, the controller comprising:

input means for receiving data from at least one detector which indicates a breach of security;

output means for outputting an alarm signal; and

computer network server means operable to interact between the security alarm controller and a computer network user who has access to the network, whereby the computer network server means is operable to pass data relating to the status of the alarm system to the network user and is operable to re-configure the alarm system controller on the basis of instructions from the network user.

2. A security alarm system controller according to claim 1, wherein the computer network server means is an Internet server means.

3. A security alarm system controller according to claim 1 or 2, the controller being re-configurable to be armed (set) or disarmed.

4. A security alarm system controller according to any one of claims 1 to 3, which, when the property which is being protected by the alarm system is divided into a plurality of zones, is re-configurable to exclude or add a zone.

5. A security alarm system controller according to any previous claim, wherein the network server means includes a telephone line connection by which the network user can access the controller.

6. A security alarm system controller according to claim 5, wherein the telephone line connection also serves as the output means, or a part of the output means.

7. A security alarm system controller according to any one of previous claims, wherein the computer network server means is accessible by a network user via a remote monitoring station.

8. A security alarm system controller according to according to any one of the previous claims, wherein the input means is arranged to receive image data from a camera.

9. A security alarm system controller according to claim 8, further comprising a camera control output for controlling the camera.

10. A security alarm system comprising:

a controller having input means for receiving data from at least one detector which indicates a breach of security, and output means for outputting an alarm signal; and

a computer network server means located as part of the controller or entirely separate therefrom which is operable to interact between the security alarm controller and a computer network user who has access to the network, whereby the network server means is operable to pass data relating to the status of the alarm system to the network user, and is operable to re-configure the alarm system on the basis of instructions from the network user.

11. A security alarm system according to claim 10, wherein the computer network server means is an Internet server means.

12. A security alarm system according to claim 10 or 11, the controller being re-configurable to be armed (set) or disarmed.

13. A security alarm system according to any one of claims 10 to 12, which, when the property which is being protected by the alarm system is divided into a plurality of zones, is re-configurable to exclude or add a zone.

14. A security alarm system according to any one of claims 10 to 13, wherein the network server means includes a telephone line connection by which the network user can access the controller.

15. A security alarm system according to claim 14, wherein the telephone line connection also serves as the output means, or a part of the output means.

16. A security alarm system according to any one of claims 10 to 15, wherein the computer network server means is located, at least in part, at a remote monitoring station.

17. A security alarm system according to claim 16, wherein the controller and the server means are each able to access a telephone line for interconnection.

18. A security alarm system according to any of claims 10 to 17, further comprising a camera for supplying image data to the controller.

19. A security alarm system according to claim 18, wherein the controller further includes means for controlling the camera.

20. A security alarm system according to any one of claims 10 to 19, further comprising means for monitoring temperature conditions, at the site of the alarm controller.

21. A security alarm system according to any one of the claims 10 to 20, further comprising a video entry telephone system which supplies video data of callers to the controller.

22. A security alarm system according to any of claims 18 to 21, further comprising means for storing image data or video data.

23. A security alarm system according to any one of claims 10 to 22, further comprising one or more microphones for supplying audio data to the controller.

24. A security alarm system constructed and arranged substantially as herein described with reference to the drawings.